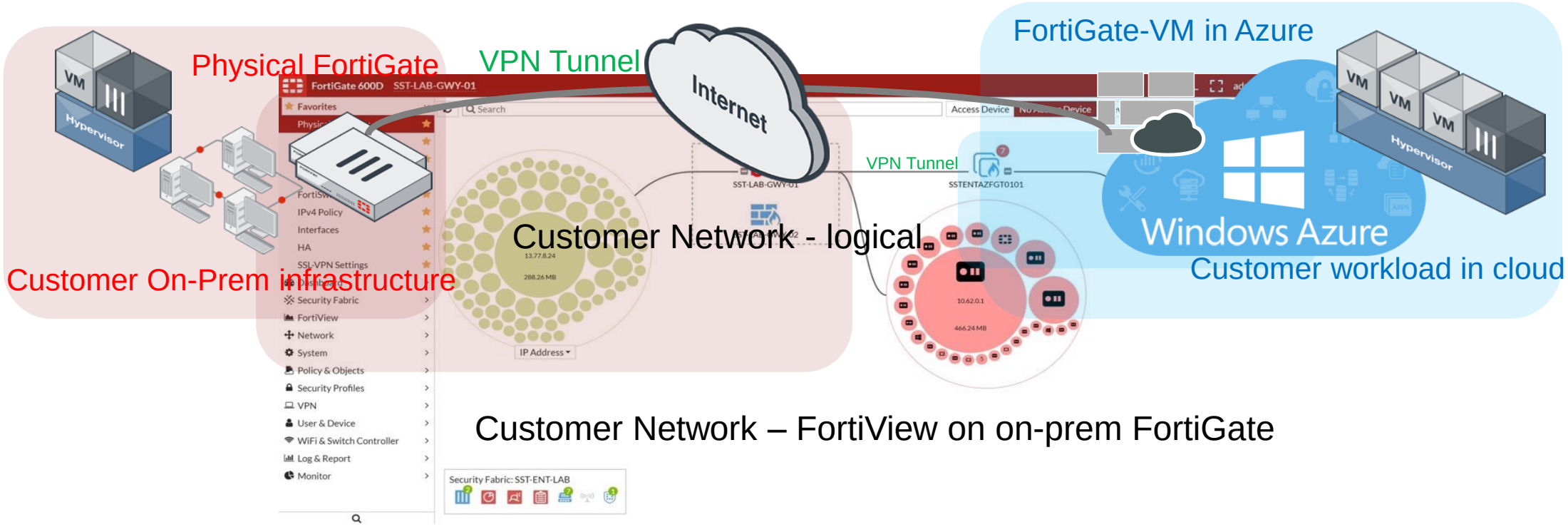
FortiGate Deployment Scenarios on Microsoft Azure

December 2017

Fortinet Security Fabric - Extending to Azure Cloud

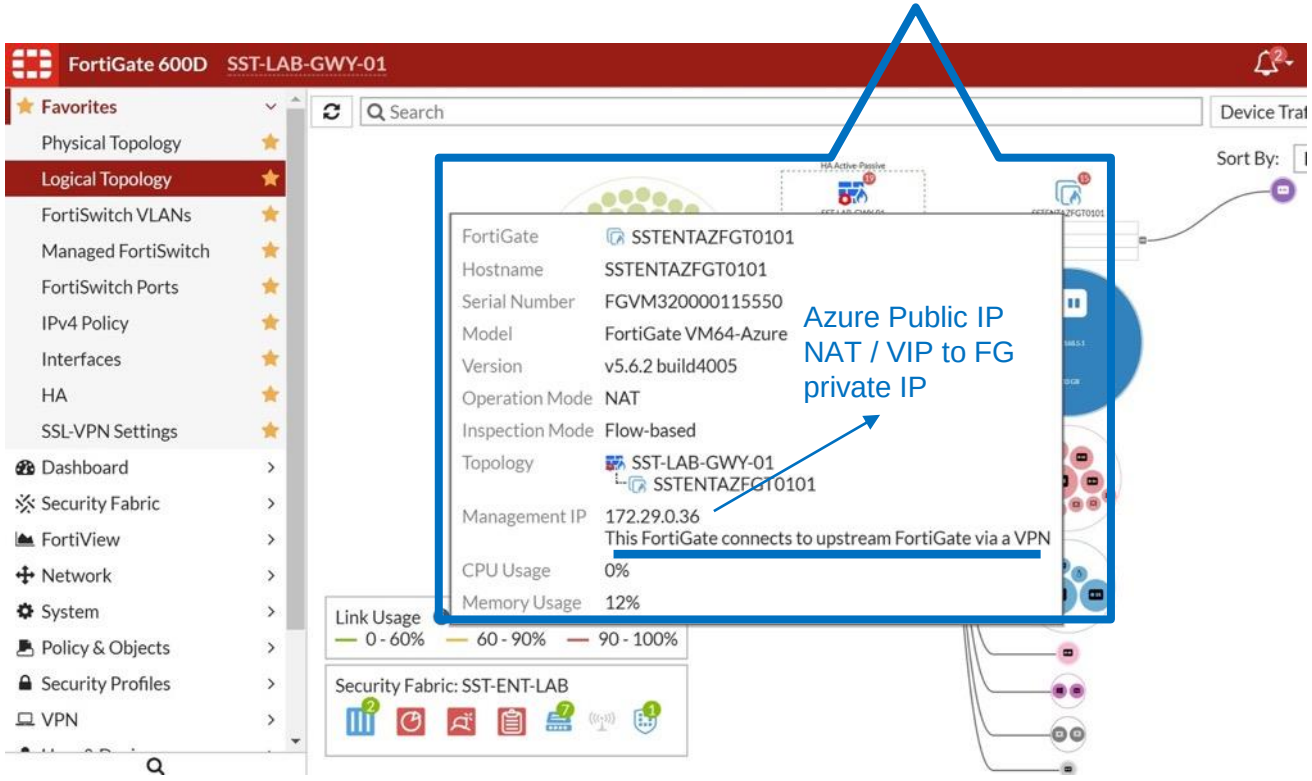
Cloud Security



Customer Network – FortiView on on-prem FortiGate

Security Fabric in Action – FortiGate instance at Azure

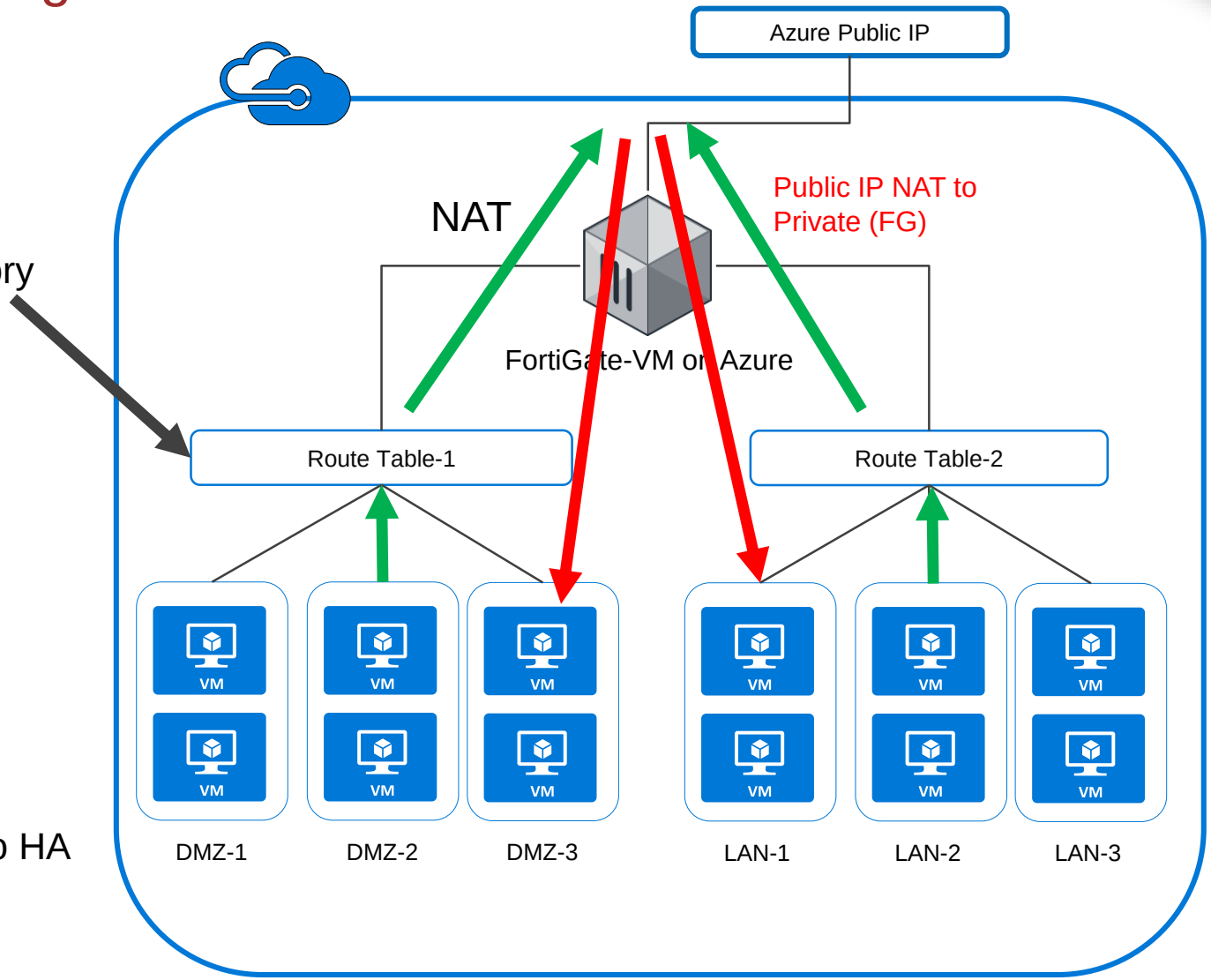
- Customer on-prem infrastructure *'extends' to cloud* via VPN
  - from on-prem FortiGate to FortiGate-VM in Azure Marketplace
- Features Supported including:
  - Fabric View
  - Fabric Audit
  - Consolidated logging
  - V-series licensing (no VDOMs)
    - Based on v5.6.2



Design Option 1 - Azure Simple Application hosting

Use Case : Application/DMZ Hosting

- Perimeter Firewalling
  - » Inbound: DNAT by Azure (red)
    - VIP on FG to allow services
    - SNAT on FG **optional**
  - » Outbound: Azure UDR/Route-table Mandatory
- Internal Segmentation
  - Traffic between DMZ/LAN via FG
  - Azure UDR/Route-table Mandatory
- Simple Deployment
  - » Single FG-VM
  - » No HA / Load balancing
  - » 99.9% Azure SLA (guaranteed by Azure)
- IPSec VPN Supported (1 to 1 NAT)
- Q: How about if FG-VM fails?
- A: Restore with backup config/license (or refer to HA design)

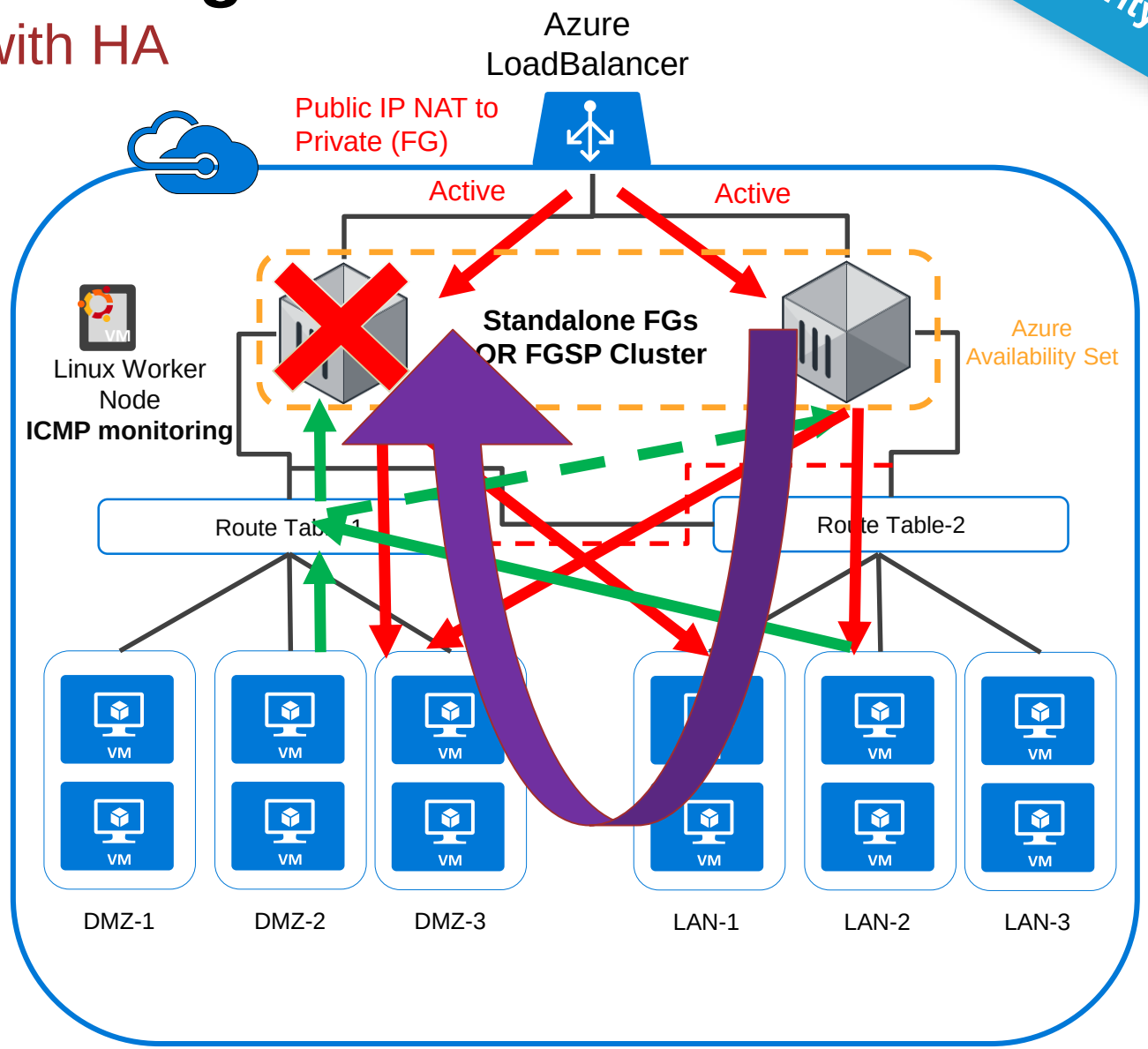


Design Option 2 – Cloud Hosting with HA

Use Case: Application/DMZ hosting with HA

- **High Availability**
  - » Inbound Active/Active (red)
  - » Outbound Active/Standby (green)
    - DMZ/LAN default route to FG1 (left)
  - » Achieved by:
    - Azure LB (in build HA)
    - Linux worker Node w/ ICMP monitoring

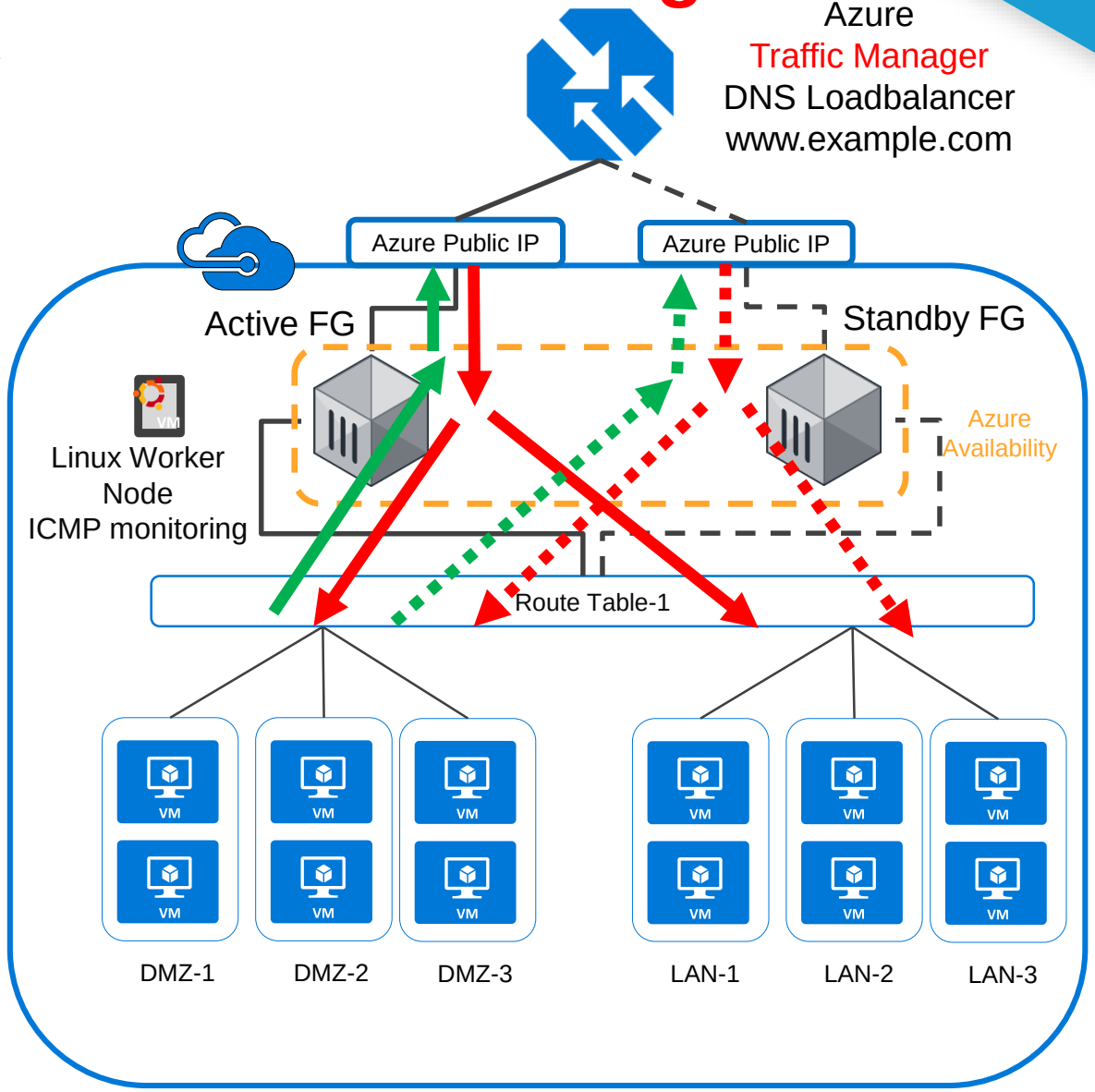
    (scripts provided by FUSE community)
  - » 2 separate “Active” FG-VMs
  - » No FGCP (traditional HA)
  - » FortiManager to maintain configs between two FGs
  - » No IPSEC VPN support (because of Azure LB)
- **Public Cloud HA**
  - » Availability Set Recommended (FG 1 & 2 on separate physical host/rack/power)
  - » FGSP Supported with **Azure Direct Server Return** (no DNAT on Azure LB, inbound)
  - » API call route-table swap/NHIP swap (Next Hop IP)
- Q: Customer lose visibility with inbound SNAT by FG
- A: if no SNAT you can end up with **Asym routing**



Design Option 3 – HA with Azure Traffic Manager

Use Case: Active/Standby Bi-directional HA

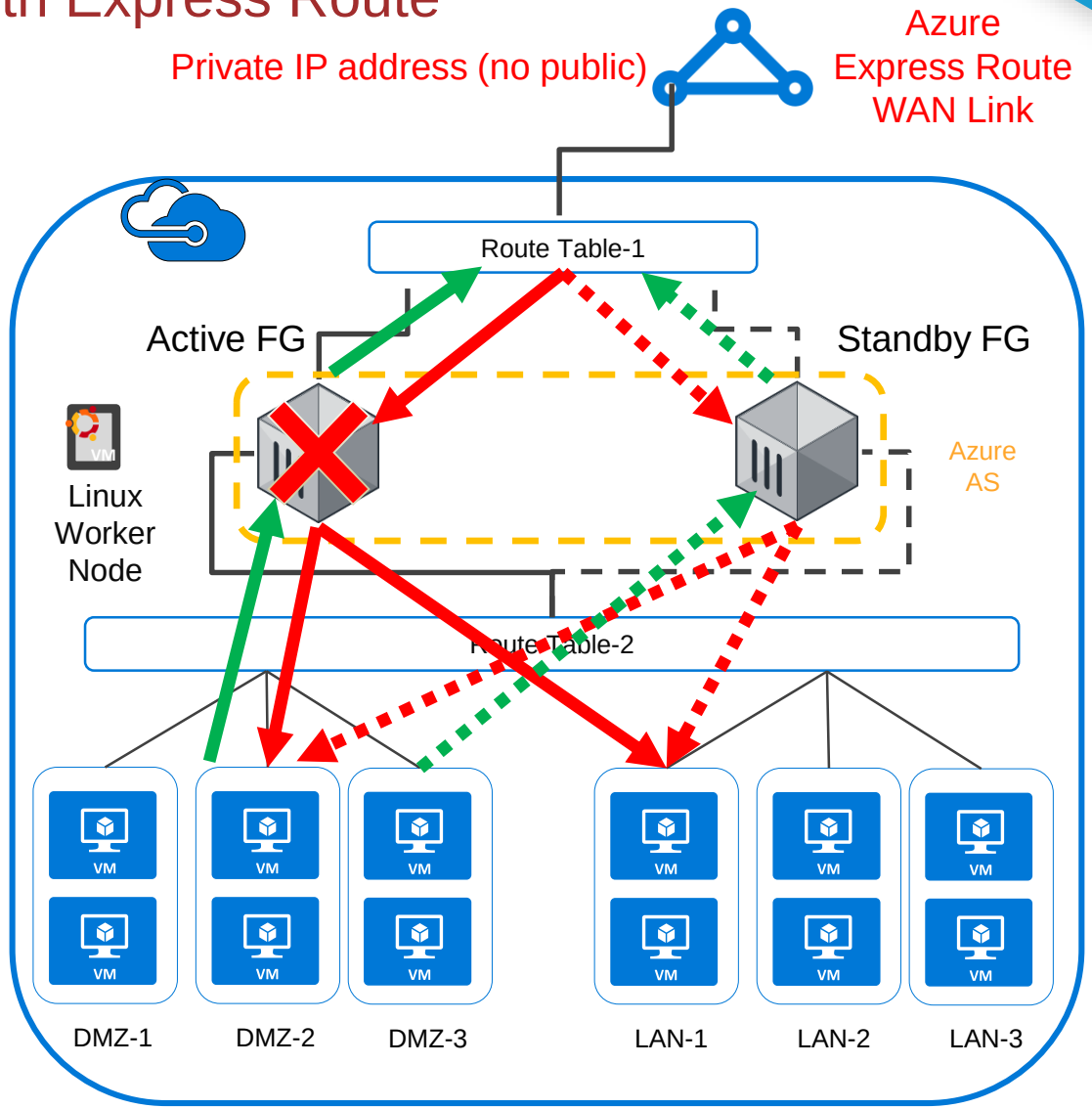
- Perimeter Firewalling
  - » DNAT by Azure (Inbound - red)
  - » SNAT on FGT optional (Outbound - green)
- Azure Traffic Manager
  - » Probe: ICMP, HTTP, frequency, etc
- Public Cloud HA
  - » Active/**Standby** (No FGCP)
  - » Linux VM / Container Controller
  - » Availability Set Recommended
- IPSec VPN Supported
- Q: When to use Azure TM?
- A: Avoid Asymmetric Route and when SNAT can't be used for return traffic.



Design Option 4 – HA with Azure Express Route

Use Case: Active/Standby Bi-directional HA with Express Route

- Azure Express Route
  - » Key: Route table(s) in front/behind FG
- Perimeter Firewalling
  - » No Nat required- Maximum visibility
  - » Inbound (red), Outbound (green)
  - » On-Prem Extension (Hybrid Cloud)
- Public Cloud HA
  - » Inbound/Outbound Active/Standby (No FGCP)
    - Only 1 NHIP from route table (can't sent to both FG),
    - ie no ECMP support
  - » FGSP support
  - » Linux VM / Container Controller
  - » Availability Set Recommended
- IPSec VPN Supported
- Q: What is different to Option 3?
  - » A: Route table used at Gateway Subnet on Express Route

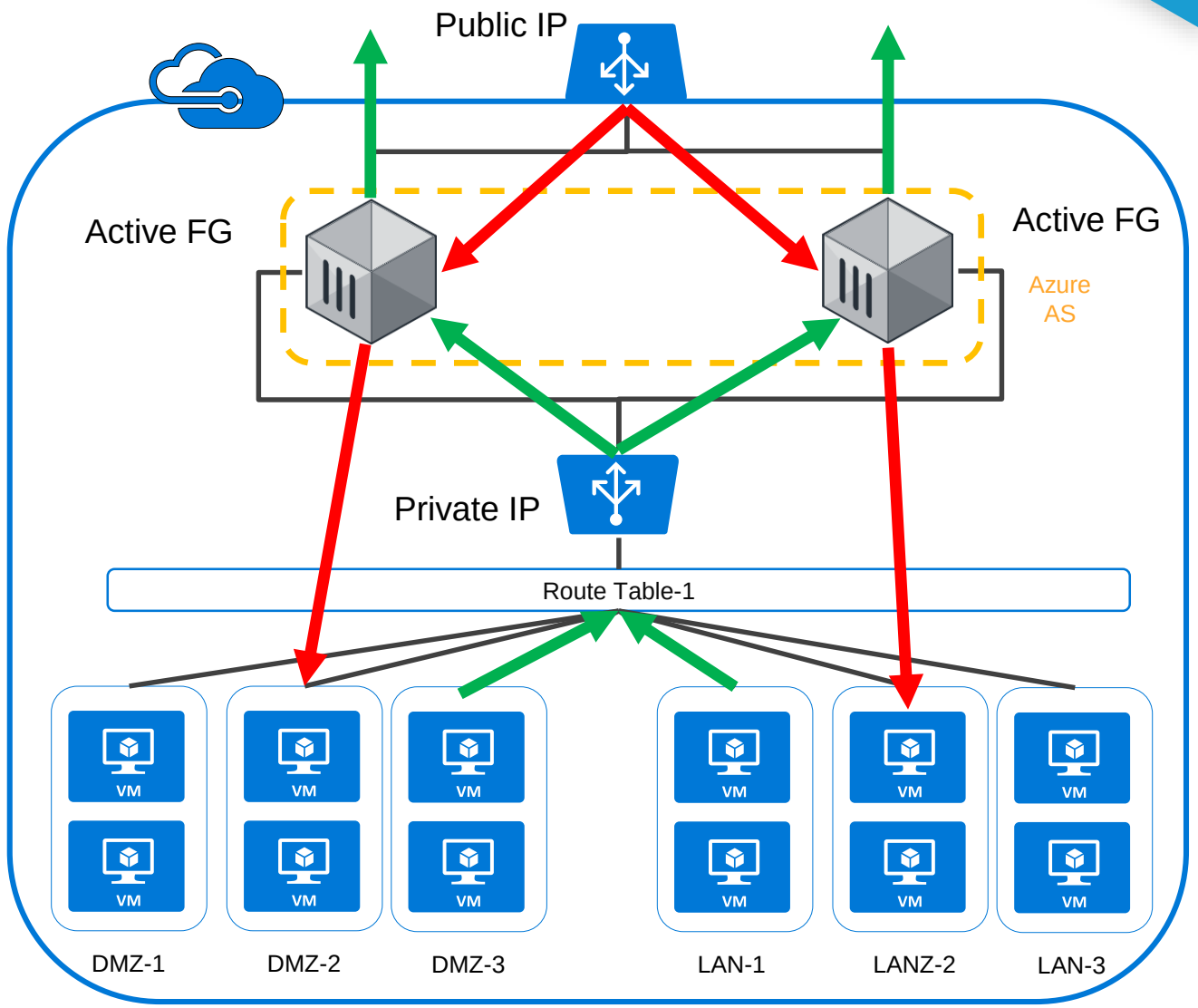


Design Option 5 – HA with Azure Internal Load Balancer

Use Case: Active/Active Bi-directional HA – Currently Under Preview

Cloud Security

- Design under review from MS (not GA)
  - » Additional internal LB (bottom one)
- Perimeter Firewalling
  - » DNAT by “public” Azure LB
  - » SNAT on FGT (Avoid Asymmetric Route
  - » NO SNAT - FGSP Works with Direct Server Return (no DNAT on Azure public LB)
  - » Internal LB – NHIP in one Route Table (vs 2 before, optional)
- Public Cloud HA
  - » **No Linux SDN controller (monitoring)**
  - » Inbound – Active/Active (red)
  - » Outbound – Active/Active (green)
  - » Availability Set Recommended
- IPSec VPN Not-Supported
- Q: Limitations?
  - » A: Only Works for TCP/UDP (All Port rule under Preview)

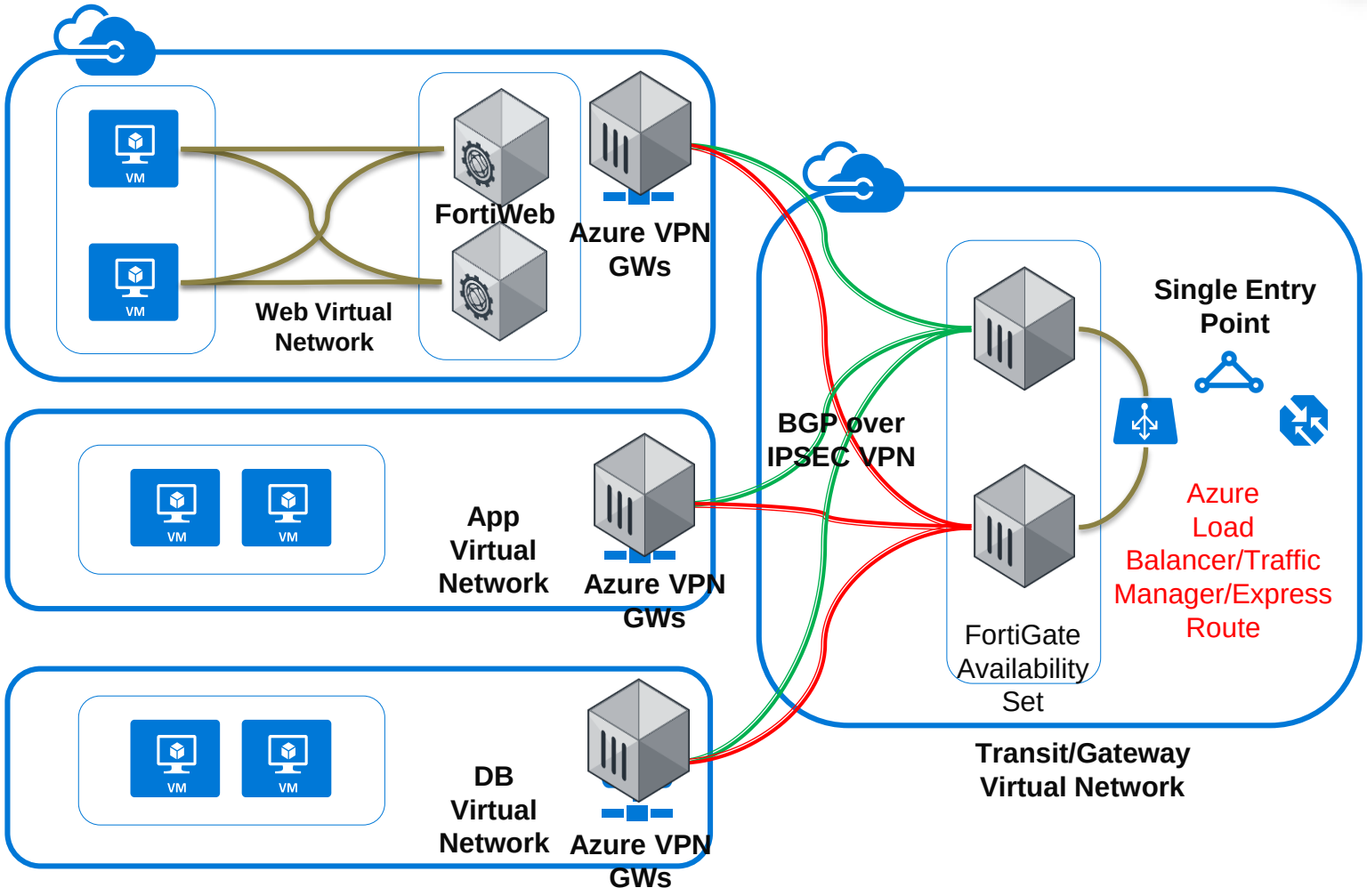


Design Option 6 – HA with IPSEC+BGP Transit vNet

Use Case: Hub and Spoke deployment, Large Enterprises

Cloud Security

- Transit Gateway Vnet
  - **Single Point of Entry into Azure Platform**
  - **Vs multiple Entry Points with FG on each vNet**
  - Auto traffic path failover with BGP
  - HA based on BGP Over IPSec VPN
  - Increases architecture complexity
  - IP NAT Pool For FGSP
- Perimeter Security
  - Reduces # of Azure FGT instances & cost by removing the requirement for 1 FortiGate per vNet, can have spoke vNet in different regions, E-W Traffic control
- Options:
  - FG Active Standby or A-A
  - Different VPN tunnel active by BGP routes (green only, green or some red)
  - Failover, all red tunnels active
  - Azure VPN GWs replaced by FG(s)
  - Active/Active(Load-Sharing Optional)



Recommended Best Practices

- Secure Gateway vNet
  - » Minimum Entry points
  - » Enforce Security at Perimeter
- Availability Sets (Azure separate power, rack, compute)
- Sizing
  - » Price Performance combination
    - Stack VM04 and VM08
  - » Instance Level
  - » NIC Level
  - » VPC / vNet level
    - Dedicated Firewall
    - Perimeter vNet / VPC
    - Org Unit vNet / VPC

FG VM level	vNIC supported	Azure Instance	AWS Instance
01	2	D1, D1v2, F1, and F1s	m3.medium
02	2, 3(c4.large)	D2, D2v2, F2, and F2s	c4.large, m4.large
04	4	D3, D3v2, F4, and F4s	c4.xlarge, m4.xlarge
08	4	D4, D4v2, F8, and F8s	c4.2xlarge, m4.2xlarge
16	8	D5v2, F16, and F16s	c4.4xlarge,
32	8	D32v3, F16, and F16s	c3.8xlarge


FORTINET